Research Paper | Education | E-ISSN No : 2454-9916 | Volume : 9 | Issue : 10 | October 2023

THE DARK WEB AND TERRORISM: A NEXUS OF CRIME AND VIOLENCE

Pushpak Ugale[1], Sanyukta Patil[2]

[1,2] Department of MCA, Vidya Bharati Mahavidyalya, Amravati

ABSTRACT

This comprehensive document delves into the intricate relationship between the dark web and terrorist activities, shedding light on how extremist organizations have harnessed the anonymity and encryption capabilities of the dark web to further their agendas. The paper begins by distinguishing between the "Surface Web" and the "Deep Web," emphasizing that the vast majority of the internet, constituting about 96%, exists beyond the reach of conventional search engines and is commonly referred to as the Deep Web. The study elucidates the various ways in which terrorist organizations employ the dark web, encompassing propaganda dissemination, secure communication, fundraising through cryptocurrencies, coordination, weapon procurement, and the acquisition of technical know-how. It further explores how the dark web facilitates terrorist activities, including the illicit trade of firearms, explosives, and downloadable weapon blueprints, creating alarming security challenges. Interestingly, the paper highlights a paradoxical shift in recent years, where terrorist propaganda dissemination on the dark web has dwindled, attributing this to the extensive presence of extremist content on the "clearnet." Consequently, terrorists may have found more accessible channels to reach their target audience, rendering the dark web less appealing for propaganda distribution. The report also underscores the critical role of the dark web in disseminating instructional materials for homemade explosives and other malicious purposes, necessitating proactive counterterrorism efforts. It discusses a case where a cyber-savvy individual supported ISIS by providing technical guidance and security measures on the dark web. The paper concludes by emphasizing the need for novel techniques and measures to monitor and analyze terrorist activities on the dark web, citing projects like MEMEX and the challenges faced by security agencies. It also touches on the issue of privacy and surveillance, highlighting the efforts of government agencies like the NSA to identify users on the dark web, raising ethical concerns. In summary, this study provides a comprehensive overview of the interplay between terrorism and the dark web, addressing its multifaceted implications and the urgent need for counterterrorism strategies in this covert and complex digital realm.

KEYWORDS: Dark Web, Terrorism, Propaganda, Cryptocurrencies, Weapons, Counterterrorism

1. INTRODUCTION

The internet is utilized by individuals daily. There are two main components to the internet: the "Surface Web" and the "Deep Web". Commonly known websites such as Amazon, Wikipedia, Facebook, YouTube, etc belong to the Surface Web, which can be crawled by search engines like Google, Bing, Yahoo, and the like. This part of the internet, often referred to as the "Visible Web", only makes up 4% of the total internet that the public can access. Although the Surface web has a wealth of information and is lawful, it is not the entirety of the internet. Beyond these common websites, there are sites that are hidden; these make up approximately 96% of the internet and are not readily available to the general public. This vast hidden area is referred to as the Deep Web. Access to the data on the Deep Web such as internet banking or private accounts requires verification.

Terrorist activities have been observed on various online platforms since the late 1990s. However, it has been determined that the Surface Web poses a significant risk for terrorists seeking anonymity, as they can be easily monitored, traced, and located. Many terrorist websites and social media accounts on the Surface Web are under constant surveillance by counter-terrorism agencies and are frequently shut down or hacked. Conversely, the Dark Net provides decentralized and anonymous networks that facilitate the evasion of arrest and the closure of these terrorist platforms. According to Beatrice Berton of the European Union Institute for Security Studies, ISIS's activities on the Surface Web are now under close scrutiny, and the decision by several governments to remove or filter extremist content has compelled jihadists to seek new online safe havens on the Dark Net.

In the wake of the November 2015 attacks in Paris, ISIS has resorted to utilizing the Dark Net as a means to disseminate news and propaganda. This strategic shift appears to be an effort to shield the identities of the group's supporters and safeguard its content from potential cyber threats posed by hacktivists. This decision follows the successful dismantling of numerous websites affiliated with ISIS during the Operation Paris (OpParis) campaign, spearheaded by the decentralized hacker collective known as Anonymous. Al-Hayat Media Center, ISIS's media outlet, has shared a link and provided instructions on accessing their newly established Dark Net platform on a forum associated with the extremist group.

In April 2018, a comprehensive study conducted by the esteemed Henry Jackson Society unveiled a report titled "Terror in the Dark," shedding light on the escalating utilization of the Dark Net by terrorist organizations. The report's findings provide compelling evidence of the alarming trend wherein terrorists and extremists are increasingly establishing secure enclaves within the Dark Net. These havens serve as breeding grounds for plotting future attacks, procuring financial resources, and expanding their ranks through recruitment efforts.

2. HOW TERRORIST USE DARK WEB

Terrorist organizations and extremist groups have increasingly turned to the dark web as a means to advance their activities, capitalizing on its anonymity and encryption capabilities to carry out a range of actions. The following are several ways in which terrorists utilize the dark web:

1. Propaganda and Recruitment: The dark web serves as a platform for terrorist organizations to disseminate propaganda materials, such as videos, articles, and social media posts. These materials are strategically designed to radicalize individuals and recruit new members

2. Secure Communication: The dark web provides secure communication channels that pose significant challenges for law enforcement and intelligence agencies in terms of monitoring. Terrorists employ encrypted messaging services and anonymous email platforms to communicate, plan operations, and share sensitive information.

3. Funding and Financial Transactions: Cryptocurrencies are frequently employed for financial transactions on the dark web. Terrorist groups utilize these digital currencies to raise funds for their activities, collect donations, and launder money, with Bitcoin being a commonly used cryptocurrency. The pseudonymous nature of these transactions makes them difficult to trace.

Example of a TOR gun vendor website

TahrerSham website that redirects visitors to the .onion domain

4. Coordination: The dark web offers a platform for terrorists to coordinate their activities. They can discuss attack plans, share operational details, and collaborate on various projects while maintaining a high level of anonymity. Forums and chat rooms on the dark web facilitate this coordination.

5. Weapon Procurement: In certain instances, terrorists may seek to acquire weapons and explosives through dark web channels. While this aspect is not exclusive to terrorism and encompasses various forms of criminal activity, the acquisition of weapons through illegal online marketplaces poses a significant threat when utilized by terrorists.

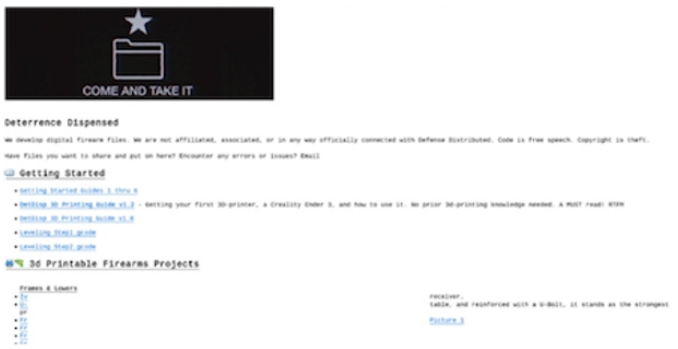
6. Technical Know-How: Extremists may access the dark web to acquire technical knowledge, including bomb-making instructions and cybersecurity skills. Online manuals and connections with like-minded individuals enable them to gain expertise in these areas.

3. THE EBBING TIDE: WHY SALAFI-JIHADIST PROPAGANDA ON THE DARK WEB DWINDLED IN 2021

The majority of digital repositories containing jihadist propaganda that operated on the dark web in recent years have been found to be absent as of the beginning of 2021. This discovery is surprising considering that Salafi-jihadist violent extremist organizations (VEOs) typically focus on reestablishing communication channels that have been blocked by law enforcement agencies. On the surface web, these organizations tend to resurface in new locations almost immediately, resembling a repetitive and tiresome game of whack-a-mole. Therefore, it begs the question as to why the same pattern is not observed on the Onion Router (TOR). The current situation suggests that terrorist organizations have largely abandoned the distribution of propaganda on the dark web, despite their high level of activity on the surface and deep web. Paradoxically, this very activity may be the primary reason. Given the significant presence of Salafi-jihadist VEOs on the "clearnet," despite years of extensive countering violent extremism (CVE) programs, there may simply be no need to disseminate manipulative releases through TOR, which had only 8 million daily users in 2018. In other words, it makes little sense to exploit the more complex and less popular dark web for this purpose when a large number of internet users are still exposed to digital jihad elsewhere.

4. FACILITATING TERRORIST ACTIVITIES WITH THE DARK WEB

The limited availability of Salafi-jihadist propaganda repositories in TOR should not be misconstrued as a lack of extensive usage by violent extremist organizations (VEOs) and their followers for other purposes. Primarily, the Onion Router has provided a conducive environment for the coordination of terrorist activities. As previously mentioned, it facilitates the illicit trade of firearms on a significant scale. Independent vendors and popular cryptomarkets serve as platforms for ordering guns. A study conducted by Paoli et al. revealed the existence of at least 18 markets that permitted gun sales in 2016.



Example of a TOR website specialized in disseminating 3D gun blueprints

Additionally, the research identified 52 active vendor accounts

during that period, estimating a monthly gross revenue of $80,000 from these transactions. Apart from firearms, ammunition and explosives have also been traded on the dark web. These transactions typically occur using cryptocurrencies such as Bitcoin (BTC) and Monero (XMR). Furthermore, these weapons are often shipped globally in a manner that evades detection at border checkpoints. Moreover, TOR hosts a plethora of weapon blueprints that can be downloaded and utilized for 3D printing, providing a potentially safer alternative for acquiring firearms necessary for carrying out terrorist attacks.

5. WHAT ARE TERRORIST DOING ON THE DARK WEB

Terrorists have increasingly turned to the Dark Net as a means of communicating in a more secure and covert manner. This trend has been noted by French Interior Minister, Bernard Cazeneuve, who has stated that the Dark Net is extensively utilized by terrorists. In fact, those responsible for recent terrorist attacks in Europe have been found to be communicating through encrypted messages on the deep web. In the aftermath of the November 2015 attacks in Paris, ISIS has also utilized the Dark Net to disseminate news and propaganda, likely in an effort to protect the identities of its supporters and safeguard its content from hacktivists.

Numerous channels are affiliated with the Islamic State, while an increasing number of channels are emerging from other major players in the global jihadi world, such as al-Qaeda in the Arabian Peninsula (AQAP), Ansar al-Sharia in Libya (ASL), Jabhat al-Nusra (JN), and Jaysh al-Islam, both in Syria. AQAP launched its own Telegram channel on September 25, 2015, and the Libyan Ansar al-Shari'ah group created its channel the following day. According to a TRAC report, membership growth for each discrete channel is staggering, with one single Islamic State channel increasing from 5,000 members to well over 10,000 within a week's time. As an ICT report concludes, terrorist organizations continue to distribute defensive guidelines and instructions, and to expand their activities on the Darknet where they claim to be better able to protect the traffic and anonymity of the organizations themselves, as well as their supporters, from the tracking software of intelligence agencies and activists who operate against terrorist organizations on the internet. However, communication is not the only exchange that poses a threat on the Dark Net. The new alarming development is the use of virtual currencies by terrorists.

6. TRAINING FOR TERRORISM

The utilization of homemade explosives remains the prevailing choice of weapon in attacks involving improvised explosive devices (IEDs). Following the bombing incident at a concert in Manchester, UK in March 2017, it was revealed that the perpetrator had accessed online resources detailing the construction of a bomb using triacetone triperoxide (TATP). Notably, instructional materials on bomb-making were readily accessible on popular platforms such as YouTube and Facebook at that time. This is of particular significance due to the increasing prevalence of TATP as the preferred explosive for IS terrorism in Europe. Its appeal lies in the fact that its ingredients can be easily obtained from common household items, including hair bleach. In fact, TATP has been consistently employed in a series of jihadist attacks across Europe, including those in Paris (November 2015), Brussels (March 2016), Manchester (May 2017), and Parsons Green, London (September 2017). For aspiring terrorists who are unable to locate these guides through conventional web search engines, the Darknet provides a convenient alternative, often through links on web forums accessible on the surface web. As an example, a 2017 RAND study discovered 208 out of 811 arms-related listings on 24 Darknet cryptomarkets were eBooks offering instructions for the production of homemade explosives or firearms.

The recent case involving an IS member who utilized his cyber skills to support the organization's cause has shed light on the extent to which material support can provide credible fodder for terrorism. Sumata Ullah, a resident of Cardiff, was convicted by British authorities in May 2017 for being a member of IS. Ullah leveraged his cyber expertise to create a "one-stop shop" that offered a vast amount of information, including expert guidance on missile systems and how to avoid detection by law enforcement. Ullah provided guided tutorials on how to use encryption programs such as Tor and PGP to hide online extremist material from law enforcement and developed mechanisms for IS to distribute its propaganda on the Darknet. Authorities confirmed that IS was actively engaged with the material, using it for "guidance" and "instruction". The CPS argued that the nature of the offenses was so serious that, if left unchecked, the actions of Sumata Ullah could have potentially facilitated further terrorist attacks either in the UK or abroad.

On January 18, 2018, a preliminary investigation was conducted on the Dream Market marketplace utilizing the Tor browser. The search yielded 1,101 outcomes for instructional material pertaining to "security", encompassing guides on drugs, fraud, hacking, and firearms usage. Notably, the Anarchist Cookbook, a publication containing instructions on bomb-making, telecommunications phreaking devices, and weapons usage, was available for purchase at a rate of BTC0.0003.

7. COUNTERING DARK NET TERRORISM

Despite the internet being accessible to the public since the 1990s, the emergence of the Dark Net has only occurred in recent years. The increasing sophistication of terrorist utilization of the Dark Net poses a significant challenge for governments, counter-terrorism agencies, and security services. In 2015, IBM's security division published a report on security threats, which highlighted the danger of cyberattacks originating from the Dark Net, utilizing Tor networks. It is evident that there is an urgent need to develop novel techniques and measures for monitoring and analyzing terrorist activities on the Dark Net. The Defense Advanced Research Projects Agency (DARPA) proposes that MEMEX, a software designed for cataloguing Deep Web sites, could provide a solution. Although initially developed for monitoring human trafficking on the Deep Web, MEMEX's principles can be applied to almost any illicit activity on the Deep Web.

In 2014, an examination of the source code within a National Security Agency (NSA) program known as XKeyscore, which was disclosed through the Edward Snowden leaks, revealed that any individual attempting to download Tor would be automatically identified, thereby granting the NSA knowledge of the identities of millions of Tor users. Tor, the predominant browser utilized by Dark Net users, is also a primary target for the National Security Agency. The responsibility of attacking Tor falls under the jurisdiction of the NSA's application vulnerabilities branch, which operates within the systems intelligence directorate (SID). According to whistleblower Edward Snowden, one successful method employed by the NSA involves exploiting the Tor browser bundle, a compilation of software programs designed to facilitate the installation and usage of the Tor software. The initial step in this process entails locating Tor users, a task accomplished through the NSA's extensive capability to monitor substantial portions of the internet. This is made possible through the agency's collaboration with telecommunications companies in the United

States.

8. CONCLUSION

To summarize, the dark web has become an increasingly significant arena for terrorist organizations and extremist groups to advance their activities. While the majority of digital repositories containing jihadist propaganda on the dark web disappeared in 2021, this shift can be attributed to the relative ease with which these groups can disseminate their content on the clearnet, reaching a larger audience. However, this does not mean that terrorists have abandoned the dark web entirely; they continue to use it for various illicit activities.

Terrorists on the dark web engage in activities such as propaganda dissemination, recruitment, secure communication, funding through cryptocurrencies, coordination, weapon procurement, and acquiring technical knowledge. The dark web offers a level of anonymity and security that poses significant challenges for law enforcement and intelligence agencies.

To counteract dark web terrorism, there is a growing need for novel techniques and measures to monitor and analyze terrorist activities on the dark web. Initiatives like MEMEX, designed for cataloging deep web sites, could be instrumental in addressing this issue. It's worth noting that government agencies, such as the NSA, have shown a strong interest in tracking dark web users, highlighting the importance of security in this context.

In essence, the utilization of the dark web by terrorists is an evolving challenge that requires constant vigilance and innovation in counter-terrorism efforts. As the dark web continues to evolve, so too must our strategies for combating the threats it poses.

REFERENCES

1. Small Wars Journal https://smallwarsjournal.com/jrnl/art/exploring-digital-jihadist-underground-onion-router-tor
2. Going Darker? The Challenge of Dark Net Terrorism https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_terrorism.pdf
3. The Dark Web: A dive into the darkest side of the Internet https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3598902
4. The Institute for National Security Studies (INSS), 2013. "Backdoor Plots: The Darknet as a Field for Terrorism", September 10, 2013.
5. Finklea, Kristin, Dark Web, special report for Congressional Research Service, 2015. Available at http://www.fas.org/sgp/crs/misc/R44101.pdf
6. Weimann, Gabriel. 2006. Terror on the Internet. Washington, DC: United States Institute of Peace; Weimann, G. 2015. Terrorism in Cyberspace: The Next Generation. New York: Columbia University Press.
7. Berton, Beatrice, 2015. "The dark side of the web: ISIL's one-stop shop?". Report of the European Union Institute for Security Studies, June 2015. Accessed March 1, 2016.
8. Malik, N. 2018. "Terror in the Dark", a report by the the Henry Jackson Society, London. URL: http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf
9. Weimann, Gabriel, 2016a. "Going Dark: Terrorism on the Dark Web", Studies in Conflict & Terrorism 39, 195-206. URL: http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546
10. Cited in "Supporter of Extremist Group ISIS Explains How Bitcoin Could Be Used To Fund Jihad", Business Insider, July 8, 2014